Amendment to the Claims:

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

Claims 1-3: (canceled)

Claim 4 (currently amended): A system to provide a remote computing client access to resources provided by at least one server in at least one target computing network, comprising:

a point of presence node communicatively configured to connect to the at least one target computing network; and

at least one Internet Protocol Security concentrator resident in the point of presence node;

at least one access server resident in the point of presence node, wherein the at least one access server comprises a virtual private network module configured to implement a secure communication channel between the remote computing client and the at least one server in the at least one target communication network,

wherein the remote computing client comprises a virtual private network module configured to cooperate with the virtual private network module resident in the point of presence node,

wherein the virtual private network module in the remote computing client and the virtual private module in the at least one access server are configured to establish an encrypted communication channel between a specific application executing on the remote computing client and the point of presence node,

wherein the virtual private network module in the remote computing client is configured to:

generate a first encryption data set comprising a public portion and a private portion, and

transmit the public portion of the first encryption data set to the virtual private network module in the at least one access server in a first session set-up message,

wherein the virtual private network module in the at least one access server is configured to:

receive the public portion of the first encryption data set in the first session set-up message,

generate a second encryption data set corresponding to the first session set-up message, the second encryption data set comprising a public portion and a private portion,

encrypt the public portion of the second encryption data set with a private key of the at least one access server, and

transmit the encrypted public portion of the second encryption data set in a second session set-up message,

wherein the virtual private network module in the remote computing client further is configured to:

receive the encrypted public portion of the second encryption data set in the second session set-up message,

decrypt the encrypted public portion of the second encryption data set, and

if decryption is successful, establish a session between the virtual private network module in the remote computing client and the virtual private network module in the at least one access server.

Claim 5 (canceled)

Claim 6 (currently amended): The system of claim ~~5~~4, wherein:

the virtual private network module in the remote computing client communicates with the virtual private network module in the at least one access server using a message exchange mode; and

the virtual private network module in the remote computing client receives application layer data from at least one application executing on the remote computing client.

Claim 7 (previously presented): The system of claim 6, wherein the virtual private network module in the at least one access server is configured to implement a proxy client for at least one application executing on the remote computing client.

Claims 8-9 (canceled)

Claim 10 (currently amended): The system of claim ~~5~~4, wherein the remote computing device further comprises a reconfiguration system module configured to collect system configuration data relating to the remote computing device, generate a system configuration file, and stores the system configuration file in a memory module in the remote computing device.

Claim 11 (previously presented): The system of claim 10, wherein the at least one access server comprises:

a central policy manager module configured to establish configuration policies for one or more remote clients that access resources via the virtual private network module; and

a reconfiguration system module configured to cooperate with the reconfiguration system module in the remote computing device to impose configuration changes on the remote computing device.

Claim 12 (previously presented): The system of claim 10, wherein the reconfiguration system is configured to implement an atomic reconfiguration process on the remote computing device.

Claim 13 (currently amended): The system of claim ~~5~~4, wherein the remote computing device comprises a local proxy module that emulates an HTTP proxy server.

Claim 14 (previously presented): The system of claim 10, wherein the remote computing device comprises a client application tunneling module, wherein the client application tunneling module is configured to extract destination IP addresses and port numbers from communication packets and invoke the reconfiguration system module to reconfigure a name-to-address mapping for communications between the remote computing device and an application executing on a remote server.

Claim 15 (currently amended): The system of claim ~~5~~4, wherein at least one server in the point of presence node comprises a network address translation module configured to perform network address translation on incoming and outgoing packets to enable remote access to resources on one or more networks outside the at least one target computing network.

Claim 16 (previously presented): The system of claim 15, wherein the network address translation module is configured to automatically determine a network configuration for the at least one target computing network.

Claim 17 (currently amended): The system of claim ~~5~~4, wherein:

the at least one access server comprises a first network backup module;

the remote computing client comprises a second network backup module; and

the first network backup module and the second network backup module are configured to back up and restore one or more files from the at least one server.

Claim 18 (previously presented): The system of claim 17, wherein the first network backup module is configured to maintain incremental backups of files used by the remote computing client.

Claim 19 (canceled)

Claim 20 (new): A system comprising:

at least one access server including a virtual private network module configured to implement a secure communication channel between a virtual private network module resident in a remote computing client and the at least one access server,

wherein the virtual private network module in the at least one access server is configured to:

receive, from the virtual private network module resident in the remote computing client, a public portion of a first encryption data set in a first session set-up message, generate a second encryption data set corresponding to the first session set-up message, the second encryption data set comprising a public portion and a private portion,

encrypt the public portion of the second encryption data set with a private key of the at least one access server, and

transmit, to the virtual private network module resident in the remote computing client, the encrypted public portion of the second encryption data set in a second session set-up message, and

if decryption of the encrypted second public portion of the second encryption data ser is successful, establish a session with the virtual private network module in the remote computing client.